IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: MICHAEL MARCOVICI SEMYON B. MIZIKOVSKY SARVAR M. PATEL URI BLUMENTHAL	Group Art Unit: 2617 Examiner: JOEL AJAYI Conf. No.: 8267
Serial No.: 10/661,715	Atty. Dkt.: 2100.004400/ Blumenthal 1-3-31-22
Filed: SEPTEMBER 12, 2003	
For: AUTHENTICATING ACCESS TO A WIRELESS LOCAL AREA NETWORK BASED ON SECURITY VALUE(S) ASSOCIATED WITH A CELLULAR SYSTEM	CUSTOMER NO.: 46290

APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On December 6, 2007, Appellants filed a Notice of Appeal in response to a Final Office Action dated August 10, 2007, issued in connection with the above-identified application. In support of the appeal, Appellants hereby submit this Appeal Brief to the Board of Patent Appeals and Interferences. Since the Notice of Appeal for the present invention was received and stamped by the USPTO Mailroom on December 12, 2007, the two-month date for filing this Appeal Brief is February 12, 2008. This Appeal Brief is being filed on March 10, 2008, therefore, a Petition for Extension of Time Under 37 CFR § 1.136(a) for a one-month extension is requested.

An extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, therefore, this paper is to be construed as

also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of one month, up to and including, March 12, 2008, to enable this document to be timely filed. Under 37 C.F.R. § 1.17(a), it is believed a fee of $120.00 is due. The Commissioner is hereby authorized to deduct said $120.00 fee from Williams, Morgan & Amerson, P.C.'s, Deposit Account No. 50-0786/2100.004400.

Additionally, the Commissioner is authorized to deduct the fee for filing this Appeal Brief ($510.00) from Williams, Morgan & Amerson, P.C.'s, Deposit Account No. 50-0786/2100.004400. No other fee is believed to be due in connection with the filing of this document. However, should any fee under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to this document, the Commissioner is hereby authorized to deduct said fee from Williams, Morgan & Amerson, P.C.'s, Deposit Account No. 50-0786/2100.004400.

I. REAL PARTY IN INTEREST

The present application is owned by Lucent Technologies, Inc.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences of which Appellants, Appellants' legal representative, or the Assignees are aware that will directly affect or be directly affected by or have a bearing on the decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-24 are pending in the case, each of which was rejected as follows:

- Claims 1, 2, 4, 7, 8, 10, 11, 13, 20, 21 as anticipated under 35 U.S.C. §103(a) by U.S. Patent Application 2005/0154895 ***(Zhang)*** in view of U.S. Patent Application No. 2003/0096614 ***(Paila);***

- Claims 3, 5, 9, 14, 16, 17, 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Zhang*** in view of ***Paila***, and further in view of ***Bridgelall*** (U.S. Patent Application Number: 2002/10085516).

Appellants appeal each of the rejections. For the convenience of the Office, Appellants identify the claims in this appeal as claims 1-24 and are incorporated herein under the Claims Appendix.

IV. STATUS OF AMENDMENTS

After the Final Rejections, no other amendments were made to any other claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Figure 1 illustrates a communications system 100, in accordance with one embodiment of the present invention. The communications system 100 of Figure 1 allows the users of mobile terminals 102 to access a cellular system 105 and/or a wireless local area network (WLAN) system 110. Although not so limited, in the illustrated embodiment, the cellular system 105 is a Code Division Multiple Access (CDMA) system. CDMA is a "spread spectrum" technology, allowing many users to occupy the same time and frequency allocations in a given band/space.

The communications system 100 includes a home location register/authentication center (HLR/AC) 120 that controls access to the CDMA network 105 and further includes a server 130 that controls access to the WLAN network 110. In particular, the HLR/AC 120 authenticates the identity of the remote terminals 102 desiring access to the CDMA network 105, and the server 130 authenticates the identity of the remote terminals 102 desiring access to the WLAN network 110. As described in greater detail below, in accordance with one or more embodiments of the present invention, the mobile terminals 102 seeking to access the WLAN network 110 are authenticated based on security value(s) provided by the HLR/AC 120, which, as noted, is

associated with the CDMA network 105. Thus, in one embodiment, the security provision(s) or value(s) available in a cellular network (*e.g.,* CDMA network 105) may be employed to authenticate users desiring access to the WLAN network 110. In this manner, the security values (or some form of these parameters) that are utilized to authenticate access to the CDMA network 105 may also be utilized to authenticate the users desiring access to the WLAN network 110. This capability allows the service provider to readily administer or manage the key distribution for both its CDMA and WLAN subscribers.

CDMA network security protocols typically rely on a 64-bit authentication key (A-key) and the Electronic Serial Number (ESN) of the mobile terminal 102. A random binary number called RANDSSD, which is generated in the HLR/AC 120, also plays a role in the authentication procedures. The A-key is programmed into the mobile terminal 102 and is stored in the HLR/AC 120 associated with the CDMA network 105. CDMA uses the standardized Cellular Authentication and Voice Encryption (CAVE) algorithm to generate a 128-bit sub-key called the "Shared Secret Data" (SSD). The A-key, the ESN, and the network-supplied RANDSSD are inputs to the CAVE algorithm that generates the SSD key. The SDD key can be shared with roaming service providers to allow location authentication. A fresh SSD key can be generated when a mobile terminal 102 returns to the home network or roams to a different system.

In the illustrated embodiment, the mobile terminal 102 desiring access to the WLAN network 110 is authenticated via an Extensible Authentication Protocol (EAP) using a common long-term secret key (referred to as the "WKEY") that is established between the mobile terminal 102 and the server 130. As is described in the greater detail below, a private key, WKEY, is established based on the security value(s) generated by the HLR/AC 120 of the CDMA network 105. The private WKEY key, once calculated, is typically not shared with

other, remote devices (*i.e.,* not transmitted over the air). Because the access to the WLAN network 110 is achieved in the illustrated embodiment using the EAP protocol, the server 130 shown in Figure 1 is an EAP server. The EAP protocol is described in Request for Comments (RFC) 2284. Some modifications to the EAP protocol may be desired in order to authenticate access to the WLAN network 110 using the security value(s) of the CDMA network 105. It is noted that the present invention is described in the context of the EAP protocol for illustrative purposes only, and that in alternative embodiments any other suitable authentication protocols may also be employed without deviating from the spirit and scope of the invention.

Figure 2 depicts a block diagram of the mobile terminal 102 of Figure 1, in accordance with one embodiment of the present invention. The mobile terminal 102 may take the form of one of a variety of devices, including cellular phones, personal digital assistants (PDAs), laptops, digital pagers, wireless cards, and any other device capable of communicating with a cellular network (CDMA network 105 in the illustrated example) and WLAN network 110. In the illustrated embodiment of Figure 2, the mobile terminal 102 includes two modules, a cellular module 205 and a WLAN module 210. The term "module," as utilized herein, may be implemented in software, hardware, or a combination thereof.

The cellular module 205 is generally responsible for performing the requisite acts to communicate over the CDMA network 105, including performing the call processing functions once a session has been established. In the illustrated embodiment, the cellular module 205 includes a CDMA authentication (CA) application 230 for authenticating the mobile terminal user to the CDMA network 105. The CA application 230 may include the CAVE algorithm (discussed above) to generate the SSD key (*i.e.,* the secondary authentication key used to

calculate CDMA session keys). The cellular module 205 may include a control unit 232 that is communicatively coupled to a storage unit 235.

The WLAN module 210 of the mobile terminal 102 is generally responsible for allowing a user to communicate with the WLAN network 110 using any suitable protocol, such as one of the IEEE 802.11x protocols. One example of the WLAN module 210 may be a network interface card (NIC). In the illustrated embodiment, the WLAN module 210 includes a WLAN authentication (WA) application 250 for authenticating the mobile terminal user to the CDMA network 105. The WLAN module 210 may include a control unit 252 that is communicatively coupled to a storage unit 255.

Figure 3 illustrates a procedure to determine a WKEY that may be employed to authenticate a user to the WLAN network 110 of Figure 1, in accordance with one embodiment of the present invention. As is described in greater detail below, Figure 3 illustrates one embodiment of the present invention in which the SSD key that is established during the CDMA authentication process is also employed to authenticate the mobile terminal 102 to the WLAN network 110. For the purposes of describing the authentication procedure of Figure 3, it is herein assumed that the cellular module 205 (see Figure 2) of the mobile terminal 102 generates the "Shared Secret Data" (SSD) key in the process of authenticating the user to the CDMA network 105. Thus, for the purposes of describing the authentication procedure of Figure 3, it is assumed that the mobile terminal 102, as well as the HLR/AC 120 (see Figure 1), has access to the SSD key.

The authentication procedure commences with the EAP server 130 providing an identity request (at 305) to the mobile terminal 102. The mobile terminal 102 responds (at 310) with an identifier that uniquely identifies the mobile terminal 102. For example, the mobile terminal 102

may provide an identifier that includes the International Mobile Subscriber Identity (IMSI) or a temporary identity (pseudonym).

Following the response provided (at 310) by the mobile terminal 102, the mobile terminal 102 receives a start request (at 315) (*i.e.,* "Request/AUTH/Start" message) from the EAP server 130. For the purposes of this discussion, the term "AUTH" in the phrase "Request/AUTH/Start" indicates that a new transaction sub-identifier may be appended to the existing EAP protocol to support the desired functionality. Upon receiving the start request (at 315), the WLAN module 210 of the mobile terminal 102 obtains (at 317) the SSD key by initiating a local request to the cellular module 205, which, as noted above, has access to the SSD key because it was previously generated in association with the CDMA authentication process. The SSD key may then be used by the WLAN module 210 as, for example, its root key (WKEY) for authentication purposes, and, if desired, to generate session keys. In one embodiment, the WLAN module 210 may, at block 317 of Figure 3, populate the WKEY with a cryptographic transform of the SSD key before using it for its intended purpose.

The WKEY may be used by the mobile terminal 102 to establish a call session with the WLAN 110 (see Figure 1). In one embodiment, the WKEY may be repeatedly used to establish different call sessions. That is, a new WKEY is not required each time a different call session is established. For example, the WLAN module 210 may use the WKEY to determine a first session key to use in association with a first (call or data) session, and then, for another session, determine a second session key (based on the WKEY). Among other things, the session keys may be utilized to encrypt the transmitted data and decrypt the received data. Although not necessary, the WKEY may be updated or revised as desired, for example, either after an occurrence of a selected event or after the expiration of a preselected amount of time.

The mobile terminal 102 provides a Response/AUTH/Start message (at 320) to the EAP server 130. Upon receiving the start response from the mobile terminal 102, the EAP server 130 initiates a query request (at 340) to the HLR/AC 120 via an SS7 AUTHREQ message. In this request message, the EAP server 130 may provide a mobile station identifier in the form of a mobile identification number (MIN) and/or electronic serial number (ESN). The HLR/AC 120, based on the received request message, responds (at 350) to the EAP server 130 by providing the SSD key (associated with the mobile terminal 102 desiring authentication to the WLAN network 110) in an AUTHREQ message.

The EAP server 130 receives (at 360) the SSD key transmitted by the HLR/AC 120. The EAP server 130, in one embodiment, determines the WKEY by populating it with the cryptographic transform of the SSD key, much in the same manner as done by the mobile terminal 102 earlier. At this point, the EAP server 130 and the mobile terminal 102 each have access to the WKEY, which, in this embodiment, is based on the SSD key associated with the CDMA network 105. The WLAN module 210 of the mobile terminal 102 can thereafter use the WKEY to authenticate the user to the WLAN network 110 and/or also use the WKEY to generate session keys, if desired. The act of authenticating may include transmitting one or more random challenges and receiving one or more responses associated with the random challenges, where the response(s) may be determined based on applying the WKEY to the random challenge(s).

Figure 4 illustrates a procedure to determine a WKEY that may be employed to authenticate the user to the WLAN network 110 of Figure 1, in accordance with an alternative embodiment of the present invention. As is described in greater detail below, Figure 4 illustrates one embodiment of the present invention in which random challenges provided by the HLR/AC

120 are used to generate the key, WKEY, which can then be used to authenticate the mobile terminal 102 to the WLAN network 110 and/or generate session keys, if desired. In this alternative embodiment, the SSD key need not be shared with the EAP server 130.

The authentication procedure commences with the EAP server 130 providing an identity request (at 405) to the mobile terminal 102. The mobile terminal 102 responds (at 410) with an identifier that uniquely identifies the mobile terminal 102. For example, the mobile terminal 102 may provide an identifier that includes the International Mobile Subscriber Identity (IMSI) or a temporary identity (pseudonym).

Following the response provided (at 410) by the mobile terminal 102, the EAP server 130 initiates a challenge request (at 415a) to the HRL/AC 120 via an SS7 AUTHREQ message, and the HRL/AC 120 responds to that request (at 420a) with an AUTHREQ message that includes an challenge, RANDU, and a response, AUTHU. Each RANDU challenge is typically a 24-bit value, and each AUTHU response is an 18-bit value. Although not so limited, in the illustrated embodiment, the EAP server 130 requests a plurality of challenges (see 415a and 415x) from the HLR/AC 120. In response, the HLV/AC 120 provides a pair of RANDU and AUTHU values (see 420a and 420x) for each request.

Based on receiving a series of AUTHU responses, the EAP server 130 determines (at 430) a WKEY. In one embodiment, the EAP server 130 combines the received AUTHU responses according to a preselected algorithm to determine the WKEY. The number of requests for challenges presented (at 415) by the EAP server 130 to the HLR/AC 120 may depend on a variety of factors, including the length of the WKEY, the length of the AUTHU response, and/or the preselected algorithm employed to generate the WKEY. For example, if a 128-bit WKEY is desired, and the preselected algorithm generates the WKEY based on concatenating a plurality

of 18-bit AUTHU responses, then at least eight (8) requests, and thus eight (8) AUTHU responses, are needed to generate the 128-bit WKEY (*i.e.,* 18 x 8 = 144 (where some bits may be discarded or truncated)). Of course, in other embodiments, fewer or additional requests may be made, depending on the particular implementation. It should be noted that the AUTHU responses may be combined in any desirable manner to arrive at the WKEY, as along as that combination can also be derived by the mobile terminal 102.

The EAP server 130 provides (at 450) the plurality of received RANDU challenges to the mobile terminal 102. In one embodiment, the RANDU challenges may be transmitted separately to the mobile terminal 102. In an alternative embodiment, the RANDU challenges may be combined (*e.g.,* by concatenation or some other desirable method) before transmission to the mobile terminal 102. If transmitted as a combination, the mobile terminal 102 may, if desired, parse the received string to recover the plurality of RANDU challenges. Based on the received RANDU challenges, the mobile terminal 102 determines the respective AUTHU responses (at 455) using the SSD key. The SSD key, as described above, is calculable by the CA application 230 (see Figure 2) of the mobile terminal 102, and thus is available to the WA application 250. Based on the calculated AUTHU responses, the WLAN module 210 of the mobile terminal 102 determines (at 460) the WKEY using the same algorithm as employed by the EAP server 130. In the illustrated embodiment, the AUTHU responses, once they are generated by the mobile terminal 102, are not transmitted to an authentication system, such as the EAP server 130, as they may otherwise be in a conventional Unique Challenge procedure. Rather, in the illustrated embodiment, the generated AUTHU responses are used internally by the mobile terminal 102 for the purposes of, for example, determining (at 460) the WKEY.

At block 460 of Figure 4, both the EAP server 130 and the mobile terminal 102 have access to the WKEY. The WLAN module 210 of the mobile terminal 102 can thereafter use the WKEY, for example, as a root key to authenticate the user to the WLAN network 110 and/or also use the WKEY to generate session keys, if desired.

In accordance with one or more embodiments of the present invention, a procedure is provided for determining the WKEY based on one or more of the security values or values generated by the HLV/AC 120 of the CDMA network 105. Using the WKEY as the root key, for example, the mobile terminal 102 may authenticate itself to the WLAN network 110, and, if desired, generate one or more session keys. Because the WKEY is generated based on the security value(s) that are readily available in the cellular system 105, the administration task for the network operator or the service provider is simplified, as it may not be necessary for the operator or the provider to manage different keys for different networks.

The term "security value," as utilized herein, refers to one or more secure values that have some level, although not necessarily absolute level, of protection. Although not so limited, examples of "security value" may include the SSD key, a signed response associated with a random challenge, a cryptographic value calculated using a key that is not shared (*e.g.,* root key) or a key that is shared for a limited purpose (*e.g.,* SSD key). As one example, the SSD key may be a cryptographic value that is calculated using the root key (A-key), and as another example, RANDU/AUTHU (in the context of CDMA) may be cryptographic values that are calculated using the SSD key.

The term "private key," as utilized herein, refers to a key that, once calculated, is generally not shared with another device. As noted, one example of a "private key" may be the WKEY. The private key may be utilized to authenticate a mobile terminal 102 to a network (the

WLAN 110); it may be utilized to provide session security through encryption/decryption. In one embodiment, the "private key" may be utilized as a root key, if desired.

Against this general backdrop, the claims will be discussed.

Claim 1, directed to a method, calls for determining (317) a private key for a first network (110) based on at least one security value associated with a second network (105) and establishing a plurality of sessions between a mobile terminal (102) and the first network (110) using the private key. *See* Application, p.8, ll. 11-22; p.13, ll. 11-16.

Claim 11, directed to a method, calls for receiving at least one security value associated with a cellular network (105), determining (317) a private key for a wireless local area network based on the security value associated with the cellular network (105), and allowing establishment of a plurality of sessions between a mobile terminal (102) and the wireless local area network (110) using the private key. *See* Application, p.12, line 16 to p.13, line 16.

Claim 20, also directed to a method, calls for receiving, at a server (130) that is associated with a wireless local area network (110), at least one security value associated with a cellular network (105) and determining (430), using the server (130), a private key based on the at least one security value. *See* Application, p.15, ll. 4-20. Claim 20 further calls for determining, at a mobile terminal (102), a private key based on the at least one security value associated with the cellular network (105) and allowing establishment of a plurality of sessions between the mobile terminal (102) and the wireless local area network (110) using the private key determined by the mobile terminal (102). *See id.* at p. 16, line 10 to p.17, line 2; p.12, line 16 to p.13, line 16.

Note that the reference numbers listed within the claims are provided to facilitate understanding of the claims through exemplary embodiments of the invention. As such, they are

listed herein for the benefit of the Office and are not to be construed as limiting the claims in any way.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1, 2, 4, 7, 8, 10, 11, 13, 20, and 21 are unpatentable under 35 U.S.C. §103(a) by U.S. Patent Application 2005/0154895 ***(Zhang)*** in view of U.S. Patent Application No. 2003/0096614 ***(Paila)***; and
2. Whether claims 3, 5, 9, 14, 16-17, 19 and 22 are unpatentable under 35 U.S.C. 103(a) over ***Zhang*** in view of ***Paila***, and further in view of ***Bridgelall*** (U.S. Patent Application Number: 2002/10085516).

VII. ARGUMENT

A. Independent claims 1, 11 and 20 (including their dependent claims) are Allowable

1. The cited references do not teach all of the claimed features

For ease of discussion, claim 1 is addressed first. Claim 1, which is directed to a method, calls, in part, for determining a private key for a first network based on at least one security value associated with a second network. The Examiner relies on the combination of ***Zhang*** and ***Paila*** to reject claim 1 under 35 USC 103 for obviousness. Specifically, the Examiner argues that ***Zhang*** discloses determining a private key for a first network based on at least one security value associated with a second network and establishing a connection between a mobile unit and the first network using the private key, and ***Paila*** discloses establishing a plurality of sessions. *See* Final Office Action, pp. 3-4.

It is well established that, to establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach all the claimed features. *In re Royka*, 490

F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Moreover, each of the claimed features must be disclosed identically in the prior art. In the present case, the Examiner has failed to show that the cited references disclose each and every claimed feature identically. For example, although the Examiner asserts that ***Zhang*** and ***Paila*** disclose the claimed feature of "determining a private key and establishing sessions using the private key," a review of these references reveals otherwise.

The Examiner argues that the "session key" disclosed in ***Zhang*** corresponds to "private key" of claim 1, and the "3G network" in ***Zhang*** corresponds to the "second network" of claim 1. The "session key" in ***Zhang***, however, is not determined based on a security value associated with the 3G network ("second network," according to the Examiner). Rather, ***Zhang*** describes that the "session key" is created by the WLAN server (not the 3G network), and the WLAN server (not the 3G server) then transmits the key to the user device to establish a communications session. *See* ***Zhang***, ¶24 (describing that WLAN creates a session key and encrypts the session key using the public key of the user device before transmitting it to the user device). Thus, contrary to the Examiner's suggestion, the "session key" in ***Zhang*** is **not** based on a "security value" associated with the 3G network. In fact, ***Zhang*** is silent regarding private keys

Zhang does describe that the 3G network and the WLAN network have a pre-existing trust relationship. *See* ***Zhang***, ¶25. However, Zhang makes clear in ¶24 that the "session key" (which the Examiner calls the "private key") is determined by the WLAN server using the user device's public key, and is not determined based on any "security value" associated with the 3G network.

Additionally, the "session key" in ***Zhang*** is not a "private key" of claim 1. As is well-established, the claims must be construed in view of the specification. Here the specification

provides that the term "private key" refers to a key that, once calculated, is not shared with another device. *See* Patent Application, p.18, lines 10-12. The Examiner, unfortunately, simply ignores the specification, and reads the claims in a vacuum. This is clearly improper. Unlike the "private key" of claim 1, the "session key" of ***Zhang*** describes that the "session key" is created by the WLAN server and then transmitted to the user device to establish a session. *See* ***Zhang***, ¶24. Because the "session key" in ***Zhang*** is shared with another device after it is determined (in this case with the user device), the "session key" is not a "private key" as that term is used in the claims and the specification.

The Examiner suggests that ***Paila*** teaches the claimed feature of establishing a plurality of sessions between a mobile terminal and the wireless local area network. *See* Final Office Action, p.4. Specifically, the Examiner argues that ***Paila*** describes a mobile unit establishing communications with more than one bearer network ("BN") wherein each network connection contains more than one **channel**. *See* ***Paila***, Abstract & ¶32. By this argument, the Examiner suggests that a "channel," as referred to in ***Paila***, is equivalent to a "session" as taught in claim 1. Applicants respectfully assert that the Examiner has misapplied the meaning of the term "channel." A "session" (*e.g.,* a connection between a mobile unit and a network) may utilize many different "channels" inherent in mobile wireless communications. For example, mobile wireless communications use forward and reverse access channels (FACH/RACH), random access channels (RACH), broadcast control channels (BCCH), stand-alone dedicated channels (SDCCH), and the like. Each "session" in which a mobile device connects to a network may utilize one or more of these "channels" for communication. Clearly, ***Paila*** discloses the use of multiple "**channels**", not multiple "sessions" as taught in claim 1 of the instant application. As

such, ***Paila*** does not teach the claimed feature of establishing a plurality of sessions between a mobile terminal and the wireless local area network.

In view of at least the aforementioned reasons, claim 1 (and its dependent claims) and the other pending claims are allowable. For similar reasons, claims 11 and 20 (and their respective dependent claims) are also allowable.

2. Response to Examiner's argument

In the Advisory Action, the Examiner maintains his rejection arguing that ***Zhang*** teaches the claimed feature of determining a private key for a first network based on at least one security value associated with a second network. In support, the Examiner argues that the 3G network of Zhang "determines" the private key ("session key" in Zhang, according to the Examiner). There are several problems with the Examiner's position. First, the Examiner is plainly incorrect. The session key (which the Examiner asserts corresponds to the private key of claim 1) is not "determined" by the 3G network, as the Examiner contends. Rather, Zhang describes that the WLAN network determines the "session key," and the 3G network simply forwards it to the mobile device. *See* ***Zhang***, ¶24 (stating "**WLAN server 230 provides a session key** that is encrypted with the user device public key and transmits the session key 3G network 210…[the 3G network then] transmits the session key to the user device…").

Additionally, ***Zhang*** never discloses that the "session key" is generated based on any security value of the second network (3G network, according to the Examiner) even though claim 1 of the instant Application calls for such a feature. While ***Zhang*** does describe encrypting the "session key" with a public key, this public key, however, is associated with the user device, not the second network (3G network, according to the Examiner). As such, Zhang

does not describe determining a private key based on security value associated with the second network (3G network, according to the Examiner).

3. There is no reason to combine the references

Although the Examiner relies on a combination of ***Zhang*** and ***Paila*** to reject the claims, there is no reason for one skilled in the art to combine the teachings of these references. The Examiner asserts that ***Paila*** teaches establishing multiple sessions between a mobile device and a network. A closer reading, however, reveals that ***Paila*** discloses the receiving different services on multiple **channels**, not multiple sessions as argued by the Examiner. Further, ***Paila*** is not concerned with network security or determining private keys, therefore there is no reason to combine its teachings with ***Zhang*** (*i.e.,* transitive authorization between access networks).

B. Claims 2, 12 and 21 are Allowable

1. The cited references do not teach all of the claimed features

Dependent claims 2, 12, and 21 are allowable for at least the same reasons their respective independent claims are allowable for the reasons described above. These claims are further allowable for the claimed features recited therein. For example, claim 2, which depends from claim 1, calls for determining the private key based on a shared secret data key associated with the cellular network. With respect to this feature, the Examiner argues that ***Zhang*** discloses in ¶24 determining a session key based on a shared secret data key associated with the 3G network ("cellular network," according to the Examiner). Applicants respectfully disagree. Paragraph 24 of ***Zhang*** describes that it is the WLAN server 230 that determines the session key ("private key," according to the Examiner). Notably, ***Zhang*** further describes that the session key that is generated by the WLAN server 230 is then transmitted to a user device through the 3G network. *See* ***Zhang***, ¶24. Thus, notwithstanding the Examiner's assertion to the contrary,

Zhang simply does not disclose or suggest determining the session key based on any shared secret data key associated with the 3G network. For at least this reason, Applicants submit that claim 2 is allowable. For substantially the same reasons, it is submitted that claims 12 (and its dependent claims) and 21 are also allowable.

2. Response to Examiner's argument

The Examiner argues that ***Zhang*** teaches the claimed feature of determining the private key based on a shared secret data key associated with the cellular network. *See* Advisory Action. For the Examiner's rejection to be proper, ***Zhang*** must teach this feature exactly. As explained above, however, ***Zhang*** simply does not disclose determining the private key based on a shared secret data key associated with the cellular network. A close reading actually reveals that ***Zhang*** is completely silent regarding a shared secret data key, or any other security key, associated with the cellular network. The Examiner, however, takes the position that "the session key becomes a private key after the AAA process." *See* Advisory Action. As previously stated, the "session key" is not, and does not become, a "private key." Furthermore, the Examiner's position bears no relation to an argument advocating a private key based on a **shared secret data key** associated with the cellular network. As such, the Examiner's position that ***Zhang*** teaches determining the private key based on a shared secret data key associated with the cellular network is untenable.

C. Claims 4 and 13 are Allowable

1. The cited references do not teach all of the claimed features

Claims 4 and 13 are further allowable for the features recited therein. For example, claim 4, which depends from claim 1, calls for populating the private key with a cryptographic transform of the shared secret data ("SSD") key. The Examiner alleges this feature is taught in

¶24 of ***Zhang***. The cited paragraph describes encrypting a session key using a public key of the user device. It does not, however, describe a cryptographic transform, and certainly does not describe populating the private key with such a transform of the shared secret data ("SSD") key, as called for by claim 4. For at least this reason, it is submitted that claim 4 is allowable. For substantially the same reasons, it is submitted that claim 13 is allowable.

2. Response to Examiner's argument

In the Advisory Action, the Examiner maintains that the claimed feature of for populating the private key with a cryptographic transform of the shared secret data ("SSD") key is taught by ***Zhang***. *See* Advisory Action. Specifically, the Examiner argues that the "session key" (corresponding to the "private key" of claim 1, according to the Examiner) is decrypted using the "private key." *See id.* However, for the Examiner's rejection to be proper, ***Zhang*** must teach this feature exactly. Unfortunately, the Examiner's position is incorrect. "Private keys" are not used to decrypt themselves, but they may be used to decrypt "session keys." *See* Application, p.13, ll. 11-20. Moreover, as previously stated, ***Zhang*** is completely silent regarding shared secret data keys, and ***Zhang*** does not teach the creation or population of a "private key."

D. Claims 7, 8 and 10 are Allowable

Claims 7, 8, and 10 are allowable because of the additional features recited therein. For example, claim 7, which depends from claim 1, calls for determining at least one session key based on the determined private key. The Examiner argues this feature is taught in ¶24 of ***Zhang***. The cited paragraph describes a WLAN server providing an encrypted session key to the user device where the user device, in turn, decrypts the session key using a "user device private key." *See* ***Zhang***, ¶24. The Examiner's argument fails for at least the following reasons. With respect to claim 1, the Examiner has argued the "session key" in ***Zhang*** corresponds to the

"private key" of claim 1. In the rejection of claim 7, however, the Examiner inconsistently applies this "session key" association. With respect to claim 7, the Examiner asserts that the "session key" is not the "private key," rather the "session key" is based on the "private key."

Further, in light of this reasoning, the Examiner argues that the decryption of the session key by the user device using a "user device private key" teaches the claimed feature of determining at least one session key based on the determined private key. Plainly, in ***Zhang***, the session key is not based on the private key of the user device because the session key is created by the WLAN server, and the user device private key is simply used to decrypt the session key. *See* ***Zhang***, ¶24. As such, ***Zhang*** fails to teach the claimed feature of determining at least one session key based on the determined private key. For at least this reason, it is submitted that claim 7 is allowable. For substantially the same reasons, it is submitted that claims 8 and 10 are allowable.

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application over the prior art of record. The undersigned attorney may be contacted at (713) 934-4064 with respect to any questions, comments, or suggestions relating to this appeal.

Respectfully submitted,
WILLIAMS, MORGAN & AMERSON, P.C.

Date: March 10, 2008

By: /Ruben S. Bains/
Reg. No. 46,532
10333 Richmond Dr., Suite 1100
Houston, Texas 77042
(713) 934-40
(713) 934-7011 (Facsimile)
ATTORNEY FOR APPELLANT(S)

VIII. CLAIMS APPENDIX

The claims currently under consideration, *i.e.,* claims 1-24, are listed in the Claims Appendix attached hereto.

IX. EVIDENCE APPENDIX

There is no evidence relied upon in this Appeal with respect to this section.

X. RELATED PROCEEDINGS APPENDIX

There are no related appeals and/or interferences that might affect the outcome of this proceeding.

CLAIMS APPENDIX

1. (Previously Presented) A method, comprising:

determining a private key for a first network based on at least one security value associated with a second network; and

establishing a plurality of sessions between a mobile terminal and the first network using the private key.

2. (Previously Presented) The method of claim 1, wherein the second network is a cellular network and the first network is a wireless local area network, and wherein determining the private key comprises determining the private key based on a shared secret data key associated with the cellular network.

3. (Original) The method of claim 2, wherein determining the private key based on the shared secret data key comprises applying a root key, an electronic serial number associated with the mobile terminal, and a network-supplied random value to a Cellular Authentication and Voice Encryption (CAVE) algorithm to generate the private key.

4. (Original) The method of claim 2, wherein determining the private key further comprises populating the private key with a cryptographic transform of the shared secret data key.

5. (Previously Presented) The method of claim 1, wherein the second network is a cellular network having an associated authentication center and the first network is a wireless local area network, and wherein determining the private key comprises determining the private

key based on one or more random challenges generated by the authentication center associated with the cellular network.

6. (Original) The method of claim 5, wherein the cellular network is a code division multiple access (CDMA) network, wherein determining the private key comprises determining one or more responses associated with the one or more challenges based on the shared secret data key associated with the CDMA network and combining the determined one or more responses to form the private key.

7. (Original) The method of claim 1, further comprising determining at least one session key based on the determined private key.

8. (Original) The method of claim 1, wherein establishing the plurality of sessions comprises authenticating the mobile terminal to the first network for each of the plurality of sessions.

9. (Original) The method of claim 7, wherein authenticating the mobile terminal to the first network comprises:

receiving a challenge from the first network; and

transmitting a response associated with he received challenge, wherein the response is calculated based on the private key.

10. (Original) The method of claim 1, wherein establishing the plurality of sessions comprises determining a session key for each of the plurality of sessions based on the private key.

11. (Previously Presented) A method, comprising:

receiving at least one security value associated with a cellular network;

determining a private key for a wireless local area network based on the security value associated with the cellular network; and

allowing establishment of a plurality of sessions between a mobile terminal and the wireless local area network using the private key.

12. (Original) The method of claim 11, wherein the cellular network is a code division multiple access (CDMA) network, and wherein receiving the at least one security value comprises receiving a shared secret data key associated with the CDMA network and wherein determining the private key comprises using the shared secret data key as the private key.

13. (Original) The method of claim 12, wherein determining the private key comprises populating the private key with a cryptographic transform of the shared secret data key.

14. (Original) The method of claim 12, wherein receiving the shared secret data key comprises receiving the shared secret data key over a Signaling System 7 (SS7) protocol.

15. (Original) The method of claim 12, wherein the cellular network is a code division multiple access (CDMA) network having an associated authentication center, and wherein receiving at least one security value comprises receiving one or more responses associated with one or more challenges that are generated by the authentication center associated with the CDMA network.

16. (Original) The method of claim 15, wherein receiving the one or more responses comprises receiving the one or more responses over a Signaling System 7 (SS7) protocol.

17. (Original) The method of claim 15, further comprises receiving the one or more challenges from the authentication center and providing the one or more challenges to the mobile terminal.

18. (Original) The method of claim 17, wherein providing the one or more challenges to the mobile terminal comprises providing the one or more challenges over an Extensible Authentication Protocol.

19. (Original) The method of claim 17, wherein determining the private key comprises combining the one or more responses.

20. (Previously Presented) A method, comprising:

receiving, at a server that is associated with a wireless local area network, at least one security value associated with a cellular network;

determining, using the server, a private key based on the at least one security value;

determining, at a mobile terminal, a private key based on the at least one security value associated with the cellular network; and

allowing establishment of a plurality of sessions between the mobile terminal and the wireless local area network using the private key determined by the mobile terminal.

21. (Original) The method of claim 20, wherein receiving the at least one security value comprises receiving a shared secret data key associated with the cellular network and wherein determining, at the server, comprises determining the private key based on the shared secret data key.

22. (Original) The method of claim 20, wherein receiving the at least one security value comprises receiving one or more random challenges generated by an authentication center associated with the cellular network and wherein determining, at the server, comprises determining the private key based on one or more signed responses associated with the respective one or more challenges.

23. (Original) The method of claim 20, further comprises transmitting messages between the server and the mobile terminal using an Extensible Authentication Protocol.

24. (Original) The method of claim 20, wherein determining, at a mobile terminal, the private key based on the at least one security value associated with the cellular network

comprises determining the at least one security value associated with at least one of a CDMA network, TDMA network, GSM network, OFDMA network, and AMPS network.